(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11149709 A**

(43) Date of publication of application: **02 . 06 . 99**

(51) Int. Cl **G11B 20/10**
H04H 1/02
H04L 9/28
H04N 5/91
H04N 7/16

(21) Application number: **09318188**

(22) Date of filing: **19 . 11 . 97**

(71) Applicant: **JISEDAI JOHO HOSO SYSTEM KENKYUSHO:KK**

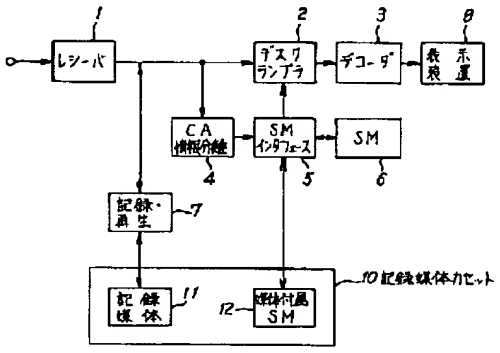
(72) Inventor: **KIMURA TAKESHI**

(54) CHARGEABLE-BROADCAST RECORDING AND REPRODUCING METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a chargeable-broadcast recording and reproducing method, in which the control of the utilization of recording, reproduction, etc., and charging corresponding to the control are carried out while ensuring integrity against malfeasance and management and treatment are facilitated.

SOLUTION: In the chargeable-broadcast transmission method, in which program signals composed of a video/video and/or various data are transmitted scrambled, CA(limited reception) information signal, in which the reception conditions of a program and a scrambling key are encrypted, is transmitted separately or multiplexed to a program signal and only receivers satisfying the reception conditions releases scrambling by the scrambling key and can use the program, a recording medium cassette 10, in which a recording medium 11 and a medium attached security module 12 are unified, is employed. The program signal, in which scrambling is executed to a recording medium 11, is recorded to the recording medium cassette while the viewing qualification information of the program is stored in the medium attached security module 12, and the program signal recorded on the recording medium is de-scrambled by a medium attached security module function at the time of reproduction.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－149709

(43)公開日　平成11年(1999)６月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｈ０４Ｈ　1/02		Ｈ０４Ｈ　1/02	Ｅ
Ｈ０４Ｌ　9/28		Ｈ０４Ｎ　7/16	Ｃ
Ｈ０４Ｎ　5/91		Ｈ０４Ｌ　9/00	６６１
7/16		Ｈ０４Ｎ　5/91	Ｐ

審査請求　有　請求項の数14　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－318188

(22)出願日　平成９年(1997)11月19日

(71)出願人　597136766
株式会社次世代情報放送システム研究所
東京都台東区西浅草１丁目１－１

(72)発明者　木村　武史
東京都台東区西浅草１丁目１番１号　株式会社次世代情報放送システム研究所内

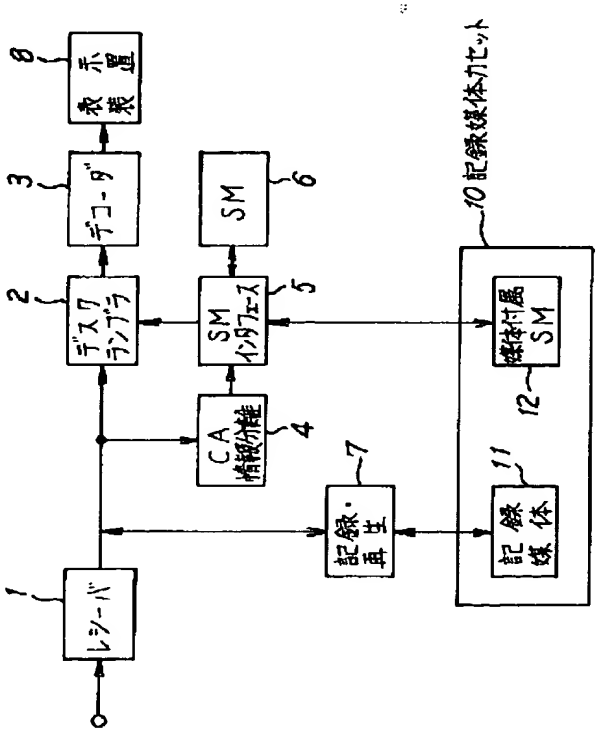
(74)代理人　弁理士　杉村　暁秀　（外８名）

(54)【発明の名称】　有料放送記録再生方法

(57)【要約】

【課題】　不正に対する完全性を確保しながら、記録・再生など利用の制御やこれに応じた課金が可能となり、さらに管理や取扱いが容易となる有料放送記録再生方法を提供する。

【解決手段】　映像・音声および／または各種データより構成される番組信号をスクランブルして伝送し、番組の受信条件およびスクランブル鍵を暗号化したＣＡ情報信号を別途または番組信号に多重して伝送し、受信条件を満たす受信者のみがスクランブル鍵によりスクランブルを解いて番組を利用できるようにした有料放送伝送方法において、記録媒体（１１）と媒体付属セキュリティモジュール（１２）とを一体化した記録媒体カセット（１０）を用い、この記録媒体カセットには、記録媒体（１１）にスクランブルを施された番組信号を記録するとともに、媒体付属セキュリティモジュール（１２）にその番組の視聴資格情報を記憶し、記録媒体に記録された番組信号は、再生時に媒体付属セキュリティモジュール機能によりデスクランブルする。



1

【特許請求の範囲】

【請求項１】　映像・音声および／または各種データより構成される番組信号をスクランブルして伝送し、番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号を別途または番組信号に多重して伝送し、利用条件を満たす受信者のみがスクランブル鍵によりスクランブルを解いて番組を利用できるようにした有料放送伝送方法において、

デスクランブラ回路、セキュリティモジュールインタフェース回路、セキュリティモジュール、記録・再生回路および記録媒体と媒体付属セキュリティモジュールを備える記録媒体カセットを有し、

記録を行なう場合にあっては、セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブルを施されたままの番組信号を記録・再生回路によって記録媒体カセットの記録媒体に記録するとともに、セキュリティモジュールインタフェース回路を介してセキュリティモジュールから記録媒体カセットの媒体付属セキュリティモジュールへ当該番組のＣＡ情報信号の暗号復号鍵および資格情報の移動または複製を行ない、

再生を行なう場合にあっては、記録媒体カセットの媒体付属セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブル鍵をデスクランブラ回路に供給することにより、記録媒体カセットの記録媒体を記録・再生回路によって再生して得られた番組信号を、デスクランブラ回路でスクランブル鍵に従ってスクランブルを解除する、ことを特徴とする有料放送記録再生方法。

【請求項２】　請求項１記載の方法において、セキュリティモジュールと記録媒体カセットの媒体付属セキュリティモジュール間で行なう情報の授受は、当該方法の受信ＣＡ情報の暗号方式と異なる暗号方式を用いることを特徴とする有料放送記録再生方法。

【請求項３】　映像・音声および／または各種データより構成される番組信号をスクランブルして伝送し、番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号を別途または番組信号に多重して伝送し、利用条件を満たす受信者のみがスクランブル鍵によりスクランブルを解いて番組を利用できるようにした有料放送伝送方法において、

デスクランブラ回路、セキュリティモジュールインタフェース回路、セキュリティモジュール、記録回路、再生回路および２組の記録媒体と媒体付属セキュリティモジュールを備える記録媒体カセットを有し、

記録を行なう場合にあっては、セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブルを施されたままの番組信号を記録回路によって記録媒体カセットの記録媒体に記録するとともに、セキュリティモジュールインタフェース回路を介してセキュリティモジュールから記録媒体カセットの媒体付属セキュリティモジュールへ当該番組のＣＡ情報信号の暗号復号鍵および資格情報の移動または複製を行ない、

再生を行なう場合にあっては、記録媒体カセットの媒体付属セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブル鍵をデスクランブラ回路に供給することにより、記録媒体カセットの記録媒体を再生回路によって再生して得られた番組信号を、デスクランブラ回路でスクランブル鍵に従ってスクランブルを解除し、

複写を行なう場合にあっては、再生側の記録媒体カセットの媒体付属セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合には再生側の記録媒体カセットの記録媒体から再生回路によって再生されたスクランブルを施された番組信号をスクランブルを施された状態のまま記録回路によって記録側の記録媒体カセットの記録媒体に記録するとともに、セキュリティモジュールインタフェース回路を介して再生側の記録媒体カセットの媒体付属セキュリティモジュールから記録側の記録媒体カセットの媒体付属セキュリティモジュールへ当該番組のＣＡ情報信号の暗号復号鍵および資格情報の移動または複製を行なう、ことを特徴とする有料放送記録再生方法。

【請求項４】　請求項３記載の方法において、セキュリティモジュールと記録媒体カセットの媒体付属セキュリティモジュール間および／または再生側の記録媒体カセットの媒体付属セキュリティモジュールと記録側の記録媒体カセットの媒体付属セキュリティモジュール間で行なう情報の授受は、当該方法の受信ＣＡ情報の暗号方式と異なる暗号方式を用いることを特徴とする有料放送記録再生方法。

【請求項５】　請求項１から４いずれか記載の有料放送記録再生方法において、前記ＣＡ情報信号を記録媒体カセットの記録媒体に記録することを特徴とする有料放送記録再生方法。

【請求項６】　請求項１から４いずれか記載の有料放送記録再生方法において、前記ＣＡ情報信号を記録媒体カセットの媒体付属セキュリティモジュールに記憶することを特徴とする有料放送記録再生方法。

【請求項７】　請求項１から６いずれか記載の有料放送記録再生方法に使用する記録媒体を備えた記録媒体カセットであって、ＣＰＵを内蔵したセキュリティモジュールを、不可分な形態もしくは装着する形態で備えることを特徴とする記録媒体カセット。

【請求項８】　請求項７記載の記録媒体カセットにおい

2

て、前記記録媒体にはスクランブルを施された番組信号および番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号が事前記録されていて、前記セキュリティモジュールには番組の利用資格が事前記憶されているとともに、ＣＡ情報信号の暗号を復号し、番組の利用条件と利用資格を検査し、条件を満足する場合にはスクランブル鍵を出力するか、またはＣＡ情報信号の暗号復号鍵および資格情報を転送する機能を備えることを特徴とする記録媒体カセット。

【請求項９】　請求項７記載の記録媒体カセットにおいて、前記記録媒体にはスクランブルを施された番組信号および番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号を記録し、前記セキュリティモジュールには番組の利用資格を外部から記憶する機能を備えるとともに、ＣＡ情報信号の暗号を復号し、番組の利用条件と利用資格を検査し、条件を満足する場合にスクランブル鍵を出力する機能を備えることを特徴とする記録媒体カセット。

【請求項１０】　請求項７記載の記録媒体カセットにおいて、前記記録媒体にはスクランブルを施された番組信号が事前記録されていて、前記セキュリティモジュールには番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号および利用資格が事前記憶されているとともに、ＣＡ情報信号の暗号を復号し、番組の利用条件と利用資格を検査し、条件を満足する場合にスクランブル鍵を出力する機能を備えることを特徴とする記録媒体カセット。

【請求項１１】　請求項７記載の記録媒体カセットにおいて、前記記録媒体にはスクランブルを施された番組信号を記録し、前記セキュリティモジュールには番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号および番組の利用資格を外部から記憶する機能を備えるとともに、ＣＡ情報信号の暗号を復号し、番組の利用条件と利用資格を検査し、条件を満足する場合にスクランブル鍵を出力する機能を備えることを特徴とする記録媒体カセット。

【請求項１２】　請求項１から６いずれか記載の有料放送記録再生方法に使用するセキュリティモジュールであって、ＣＡ情報信号の暗号を復号し、番組の利用条件と利用資格を検査し、条件を満足する場合にはＣＡ情報信号の暗号復号鍵および資格情報を転送する機能を備えることを特徴とするセキュリティモジュール。

【請求項１３】　請求項１から６いずれか記載の有料放送記録再生方法に使用するデスクランブラ回路、セキュリティモジュールインタフェース回路および記録再生回路を備えた有料放送記録再生に使用する装置であって、請求項７から１１いずれか記載の記録媒体カセットおよび請求項１２記載のセキュリティモジュールとともに用いて動作するよう構成されたことを特徴とする有料放送記録再生に使用する装置。

【請求項１４】　映像・音声および／または各種データより構成される番組信号をスクランブルして伝送し、番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号を別途または番組信号に多重して伝送し、利用条件を満たす受信者のみがスクランブル鍵によりスクランブルを解いて番組を利用できるようにした有料放送伝送方法に使用するパーソナルコンピュータ装置において、記憶機能、ＰＣ付属セキュリティモジュール、デスクランブル機能、編集機能および／または提示機能を有し、スクランブルを施された番組信号を記憶機能に、番組の利用資格をＰＣ付属セキュリティモジュールに、番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号を記憶機能またはＰＣ付属セキュリティモジュールに記録し、

ＰＣ付属セキュリティモジュールは、ＣＡ情報信号の暗号を復号し、番組の利用条件と利用資格を比較・検査し、条件を満足する場合にスクランブル鍵を出力することによって、記憶機能から読み出されたスクランブルを施された番組信号を、デスクランブル機能においてスクランブル鍵に従ってスクランブルを解除したのち、編集機能および／または提示機能において番組信号を編集および／または提示する、ことを特徴とするパーソナルコンピュータ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、映像・音声および／または各種データより構成される番組信号をスクランブルして伝送し、番組の受信条件およびスクランブル鍵を暗号化したＣＡ（Conditional Access：限定受信）情報信号を別途または番組信号に多重して伝送し、受信条件を満たす受信者のみがスクランブル鍵によりスクランブルを解いて番組を利用できるようにした有料放送伝送方法の分野に属し、特に、その放送番組を記録媒体に記録・再生して利用するような場合において、その利用を細かく制御するための方法に関するものである。

【０００２】

【従来の技術】第１の従来技術として、デスクランブルを施された番組信号を記録・再生する場合の構成略ブロック線図を図７に示す。第１の従来技術において記録する場合には、次のような動作を行なう。レシーバ回路１で受信されたスクランブルを施された番組信号はデスクランブラ回路２に入力される。一方、ＣＡ情報信号はＣＡ情報分離回路４により抽出され、セキュリティモジュールインタフェース（ＳＭインタフェース）回路５を介してセキュリティモジュール（ＳＭ）６に入力される。そこで、セキュリティモジュール６ではＣＡ情報信号を暗号復号し、利用条件を満足しているか否か判定した後スクランブル鍵をデスクランブラ回路２に渡す。番組信号はデスクランブラ回路２においてスクランブル鍵に従ってスクランブルを解除される。スクランブルを解除さ

れた番組信号は記録・再生回路７によって記録媒体１１に記録される。

【０００３】再生する場合には、記録媒体カセットの記録媒体１１を記録・再生回路７によって再生することによりスクランブルを解除された番組信号が得られる。このスクランブルを解除された番組信号はデコーダ回路３でデコードされて表示装置８に提示される。

【０００４】この方法では、記録媒体にスクランブルを解除された番組信号を透明に記録・再生するため、一旦スクランブルを解除された番組信号はいくらでも記録可能であり、それは再生すれば直ちに視聴可能であり、さらに複製を作ることも可能である。このように、第１の従来技術では番組の記録や複製を制御するすべを全く持たない。

【０００５】第２の従来技術として、第１の従来技術に加えてＣＧＭＳ（Copy GenerationManagement System）技術を用いる場合の構成略ブロック線図を図８に示す。ＣＧＭＳ技術とは、２ビットのＣＧＭＳ信号を用いて、「００」の場合「制約条件なしにコピー可」、「１０」の場合「１世代のみコピー可」、「１１」の場合「コピー禁止」、を指示することによってコピーの世代制御を行なう技術である。

【０００６】この第２の従来技術において記録する場合には次のような動作を行なう。レシーバ回路１で受信されたスクランブルを施された番組信号はデスクランブラ回路２に入力される。一方、ＣＡ情報信号はＣＡ情報分離回路４により抽出され、セキュリティモジュールインタフェース回路５を介してセキュリティモジュール６に入力される。そこで、セキュリティモジュール６ではＣＡ情報信号を暗号復号し、利用条件を満足しているか否か判定した後スクランブル鍵をデスクランブラ回路２に渡す。番組信号はデスクランブラ回路２においてスクランブル鍵に従ってスクランブルを解除される。ここまでの動作は第１の従来技術の場合と同じである。次に、スクランブルを解除された番組信号はＣＧＭＳ制御回路９においてＣＧＭＳ信号を検査される。ＣＧＭＳ信号が「００」の場合は記録・再生回路７によって記録媒体１１に記録され、ＣＧＭＳ信号が「１１」の場合には記録は禁止される。また、ＣＧＭＳ信号が「１０」の場合はＣＧＭＳ信号を「１１」に書き換えた後、記録・再生回路７によって記録媒体１１に記録される。これによって次の世代のコピーは禁止される。

【０００７】再生する場合には、記録媒体カセットの記録媒体１１を、記録・再生回路７によって再生することによりスクランブルを解除された番組信号が得られる。このスクランブルを解除された番組信号はデコーダ回路３でデコードされて表示装置８に提示される。

【０００８】この方法では、「制約条件なしにコピー可」「１世代のみコピー可」「コピー禁止」のように、コピー世代の制御が可能になる。しかし、コピー世代制御以外の利用制御（例えば、視聴回数、視聴期限、コピー数の制御など）を行なったり、これらの利用制御と課金を関係付けたりすることはできない。また、ＣＧＭＳ信号を書き換えることにより制御を無効化することが可能であったり、ＣＧＭＳ信号の如何に関わらず記録媒体の単純コピーを行なうことによっていくらでも複製が可能であったり、安全性の点でも課題がある。

【０００９】第３の従来技術として、スクランブルを施された状態のままの番組信号を記録・再生する場合の構成略ブロック線図を図９に示す。第３の従来技術において記録する場合には、受信した番組信号はスクランブルを施された状態のまま、記録・再生装置の記録・再生回路７によって記録媒体１１に記録される。

【００１０】再生を行なう場合には次のような動作を行なう。記録媒体カセットの記録媒体１１を、記録・再生回路７によって再生し、記録時の状態と同じスクランブルを施された番組信号を得る。このスクランブルの施された番組信号はデスクランブラ回路２に入力される。ＣＡ情報信号は番組信号とともに記録・再生回路７によって再生され、ＣＡ情報分離回路４により抽出されたのち、セキュリティモジュールインタフェース回路５を介してセキュリティモジュール６に入力される。そこで、セキュリティモジュール６では、ＣＡ情報信号を暗号復号し利用条件を満足しているか否か判定した後スクランブル鍵をデスクランブラ回路２に渡す。番組信号はデスクランブラ回路２においてスクランブル鍵に従ってスクランブルを解除され、デコーダ回路３でデコードされて表示装置８に提示される。

【００１１】この方法では、記録媒体にはスクランブルを施されたままの番組信号を記録しているため、仮に記録媒体の単純コピーを行なったとしても、セキュリティモジュールがなければ番組を視聴することはできないため安全性の点で改善されている。また、再生・視聴時にセキュリティモジュールを使用するため、このセキュリティモジュールの関与する範囲で細かな利用制御を行なったり、これらの利用制御と課金を関係付けたりすることも可能になる点でも改善される。

【００１２】しかし、ある番組を記録した記録媒体とその番組の視聴資格が記憶されたセキュリティモジュールとは、必ず対で扱わないとこれらの制御機能は有効に働かない。したがって、対の関係にある記録媒体とセキュリティモジュールとはその関係が分かるように管理する必要がある。ある期間使用しているセキュリティモジュールは、その期間に記録した複数の記録媒体と対の関係にあるためその管理は大変面倒である。

【００１３】

【発明が解決しようとする課題】第２の従来技術では、２ビットのＣＧＭＳ信号によって単純に複製世代の状態を示すのみであるため、

①複製世代以外の制御はできない。

②不正に対する安全性がない（ＣＧＭＳ信号の改竄が容易）。
③課金の制御を行なうことができない（技術的に可能でも安全性がないので）。第３の従来技術では、番組信号を記録した記録媒体とその番組の利用資格を有するセキュリティモジュールを対で使用しなければ番組の再生利用ができないため、
④携帯に不便である（記録媒体とセキュリティモジュールの双方を携帯する必要）。
⑤再生権を紛失する危険がある（セキュリティモジュールの紛失の可能性）。また、１つのセキュリティモジュールは複数の記録媒体に記録される複数の番組の利用資格を持つことになるため、
⑥記録媒体を独立して利用することができない（譲渡や一時的な貸借に不便）。
⑦利用資格がオーバフローしてしまう可能性がある。といった問題がある。

【００１４】このような従来技術に対して、本発明は以下の条件を同時に満足する有料放送記録再生方法の提供を目的とする。
・視聴回数、視聴期限、複製数、など細かな利用の制御が可能になること。
・これらの制御に関連づけた課金も可能になること。
・以上の制御は不正に対して安全であること。
・記録媒体の管理が複雑にならないこと。

【００１５】
【課題を解決するための手段】この目的を達成するため本発明第１の有料放送記録再生方法は、映像・音声および／または各種データより構成される番組信号をスクランブルして伝送し、番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号を別途または番組信号に多重して伝送し、利用条件を満たす受信者のみがスクランブル鍵によりスクランブルを解いて番組を利用できるようにした有料放送伝送方法において、デスクランブラ回路、セキュリティモジュールインタフェース回路、セキュリティモジュール、記録・再生回路および記録媒体と媒体付属セキュリティモジュールを備える記録媒体カセットを有し、記録を行なう場合にあっては、セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブルを施されたままの番組信号を記録・再生回路によって記録媒体カセットの記録媒体に記録するとともに、セキュリティモジュールインタフェース回路を介してセキュリティモジュールから記録媒体カセットの媒体付属セキュリティモジュールへ当該番組のＣＡ情報信号の暗号復号鍵および資格情報の移動または複製を行ない、再生を行なう場合にあっては、記録媒体カセットの媒体付属セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブル鍵をデスクランブラ回路に供給することにより、記録媒体カセットの記録媒体を記録・再生回路によって再生して得られた番組信号を、デスクランブラ回路でスクランブル鍵に従ってスクランブルを解除する、ことを特徴とするものである。

【００１６】また、本発明第２の有料放送記録再生方法は、映像・音声および／または各種データより構成される番組信号をスクランブルして伝送し、番組の利用条件およびスクランブル鍵を暗号化したＣＡ情報信号を別途または番組信号に多重して伝送し、利用条件を満たす受信者のみがスクランブル鍵によりスクランブルを解いて番組を利用できるようにした有料放送伝送方法において、デスクランブラ回路、セキュリティモジュールインタフェース回路、セキュリティモジュール、記録回路、再生回路および２組の記録媒体と媒体付属セキュリティモジュールを備える記録媒体カセットを有し、記録を行なう場合にあっては、セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブルを施されたままの番組信号を記録回路によって記録媒体カセットの記録媒体に記録するとともに、セキュリティモジュールインタフェース回路を介してセキュリティモジュールから記録媒体カセットの媒体付属セキュリティモジュールへ当該番組のＣＡ情報信号の暗号復号鍵および資格情報の移動または複製を行ない、再生を行なう場合にあっては、記録媒体カセットの媒体付属セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合にはスクランブル鍵をデスクランブラ回路に供給することにより、記録媒体カセットの記録媒体を再生回路によって再生して得られた番組信号を、デスクランブラ回路でスクランブル鍵に従ってスクランブルを解除し、複写を行なう場合にあっては、再生側の記録媒体カセットの媒体付属セキュリティモジュールはＣＡ情報信号を暗号復号し、得られた利用条件を利用資格と比較・検査し、条件を満足している場合には再生側の記録媒体カセットの記録媒体から再生回路によって再生されたスクランブルを施された番組信号をスクランブルを施された状態のまま記録回路によって記録側の記録媒体カセットの記録媒体に記録するとともに、セキュリティモジュールインタフェース回路を介して再生側の記録媒体カセットの媒体付属セキュリティモジュールから記録側の記録媒体カセットの媒体付属セキュリティモジュールへ当該番組のＣＡ情報信号の暗号復号鍵および資格情報の移動または複製を行なう、ことを特徴とする。

【００１７】
【発明の実施の形態】本発明では、記録媒体と媒体付属セキュリティモジュールとを一体化した記録媒体カセットを用いる。この記録媒体カセットには、記録媒体にスクランブルを施された番組信号を記録するとともに、媒

体付属セキュリティモジュールにその番組の視聴資格情報を記憶する。記録媒体に記録された番組信号は、再生時に媒体付属セキュリティモジュール機能によりデスクランブルされ視聴可能な状態になる。

【００１８】こうすることによって、再生時にセキュリティモジュールが関与することになるため、利用時のきめ細やかな制御やこれに関連づけた課金が可能になる。これら制御の判定はセキュリティモジュール内で行ない、セキュリティモジュールに入出力される信号には暗号を用いるので不正に対する安全性が高い。また、仮に記録媒体の単純コピーを行なったとしても、セキュリティモジュールのコピーは事実上不可能であるため不正コピーに対しても安全性が高い。さらに、スクランブルを施された番組信号が記録された記録媒体と、その番組の視聴資格情報を記憶したセキュリティモジュールとは記録媒体カセットとして一体化されているので、管理や取り扱いが容易である。

【００１９】

【実施例】以下添付図面を参照し実施例により発明の実施の形態を詳細に説明する。本発明の基本構成略ブロック線図を図１に示す。基本構成では、レシーバ回路１、ＣＡ情報分離回路４、デスクランブラ回路２、デコーダ回路３、セキュリティモジュールインタフェース回路５、セキュリティモジュール６および記録・再生回路７を備える。また、記録媒体１１と、媒体付属セキュリティモジュール１２を備えた記録媒体カセット１０を用いることが特徴である。ここで、セキュリティモジュール６および媒体付属セキュリティモジュール１２は、ＣＰＵを内蔵し暗号演算機能や条件検査機能を持ったものである。なお、レシーバ回路１、ＣＡ情報分離回路４、デコーダ回路３が受信機筐体の内部に含まれているか否かは本発明の価値に影響するものではない。同様に、記録・再生回路７が記録・再生装置として受信機と別体となっているか受信機筐体に一体となっているかは本発明の価値に影響するものではない。

【００２０】まず、基本構成において通常の視聴を行なう場合について、図１に視聴時の信号の流れを反映した図２を用いて説明する。レシーバ回路１、ＣＡ情報分離回路４などを介して得られるＣＡ情報信号は、セキュリティモジュールインタフェース回路５を介してセキュリティモジュール６に入力される。セキュリティモジュール６ではＣＡ情報信号を暗号復号し得られた利用条件をセキュリティモジュール６の持つ利用資格と比較・検査し、条件を満足している場合にはスクランブル鍵をデスクランブラ回路２に渡す。一方、レシーバ回路１で受信されたスクランブルを施された番組信号は、デスクランブラ回路２においてスクランブル鍵に従ってスクランブルを解除され、デコーダ回路３でデコードされて表示装置８に提示される。この場合の動作は、従来の有料放送システムと同様である。なお、ＣＡ情報は様々な伝送形態が考えられ、ここに示すような番組信号に多重して伝送する方法はその１例である。

【００２１】次に、基本構成において記録を行なう場合について、図１に記録時の信号の流れを反映した図３を用いて説明する。まず、レシーバ回路１、ＣＡ情報分離回路４などを介して得られるＣＡ情報信号は、セキュリティモジュールインタフェース回路５を介してセキュリティモジュール６に入力される。セキュリティモジュール６では、ＣＡ情報信号を暗号復号し、得られた利用条件をセキュリティモジュール６の持つ利用資格と比較・検査し、条件を満足している場合には以下の動作を行なう。

【００２２】レシーバ回路１で受信された番組信号は、スクランブルを施された状態のまま、記録・再生回路７によって記録媒体カセット１０の記録媒体１１に記録される。ＣＡ情報信号は、番組信号とともに記録媒体カセット１０の記録媒体１１に記録されるか、またはＣＡ情報分離回路４により抽出され、セキュリティモジュールインタフェース回路５を介して記録媒体カセット１０の媒体付属セキュリティモジュール１２に記憶される。同時に、セキュリティモジュールインタフェース回路５を介して、セキュリティモジュール６から記録媒体カセットの媒体付属セキュリティモジュール１２へ、当該番組ＣＡ情報信号の暗号復号鍵や資格情報の移動または複製を行なう。このとき必要に応じて、当該記録に伴う課金の情報をセキュリティモジュール６に記憶する。

【００２３】最後に、基本構成において再生を行なう場合について、図１に再生時の信号の流れを反映した図４を用いて説明する。記録媒体カセットの記録媒体１１を、記録・再生回路７によって再生し、記録時の状態と同じスクランブルを施された番組信号を得る。このスクランブルを施された番組信号はデスクランブラ回路２に入力される。ＣＡ情報信号が番組信号とともに記録媒体カセット１０の記録媒体１１に記録された場合には、ＣＡ情報信号は番組信号とともに記録・再生回路７によって再生され、ＣＡ情報分離回路４により抽出されたのち、セキュリティモジュールインタフェース回路５を介して記録媒体カセット１０の媒体付属セキュリティモジュール１２に入力される。一方、ＣＡ情報信号が記録媒体カセット１０の媒体付属セキュリティモジュール１２に記憶された場合には、既に媒体付属セキュリティモジュール１２はＣＡ情報信号を持っている。そこで、媒体付属セキュリティモジュール１２では、ＣＡ情報信号を暗号復号し、得られた利用条件をセキュリティモジュール６の持つ利用資格と比較・検査し、条件を満足している場合にはスクランブル鍵をデスクランブラ回路２に渡す。このとき必要に応じて、当該再生に伴う課金の情報はセキュリティモジュール６に記憶する。番組信号はデスクランブラ回路２においてスクランブル鍵に従ってスクランブルを解除され、デコーダ回路３でデコードされ

て表示装置８に提示される。

【００２４】これらの動作において、セキュリティモジュール６および媒体付属セキュリティモジュール１２に入出力される信号には暗号化を施す。そのうち、ＣＡ情報信号は伝送のために限定受信システムにおいて暗号化が施されているので、これをそのまま用いればよい。セキュリティモジュール６と媒体付属セキュリティモジュール１２の間で授受される信号は、少なくとも前記ＣＡ情報信号とは異なる暗号鍵を用いる必要がある。さらには、前記限定受信システムの暗号方式とは異なる暗号方式を用いることが安全性の点からは望ましい。

【００２５】なお、記録媒体１１としては、磁気記録テープ、磁気ディスク、光磁気ディスクなどが考えられる。また、例えば磁気ディスクでも、媒体のみをカセット化したフロッピーディスク様のものでも、磁気ヘッドや記録・再生回路を含めて一体化したハードディスクドライブ様のものであってもよい。一方、媒体付属セキュリティモジュール１２としては、ＩＳＯ－７８１６に定められるＩＣカードに用いられる様なＣＰＵチップをはじめとして、非接触インタフェースを持ったセキュリティモジュールなども考えられる。これらの組み合わせに従って、記録媒体カセット１０には多くの可能な形態が存在する。

【００２６】本発明の第２の実施例として、記録媒体カセットから記録媒体カセットへ番組信号の複写を行なうことのできる場合の構成略ブロック線図を図５に示す。図１の基本構成に、記録媒体２１と媒体付属セキュリティモジュール２２を備えた記録媒体カセット２０および記録・再生回路１７を追加したものである。記録媒体カセット１０から記録媒体カセト２０の向きに複写を行なう場合の動作を以下に説明する。この場合、記録・再生回路７は再生動作を、記録・再生回路１７は記録動作を行なうことになる。

【００２７】記録媒体カセット１０の記録媒体１１を記録・再生回路７によって再生しスクンブルを施された番組信号を得る。この番組信号は、スクンブルを施された状態のまま、記録・再生回路１７によって記録媒体カセット２０の記録媒体２１に記録される。さらに、ＣＡ情報信号が番組信号とともに記録媒体に記録されている場合には、ＣＡ情報信号は番組信号とともに記録・再生回路７によって再生され、ＣＡ情報分離回路４により抽出されたのち、セキュリティモジュールインタフェース回路５を介して記録媒体カセット１０の媒体付属セキュリティモジュール１２に入力される。一方、ＣＡ情報信号が記録媒体カセット１０の媒体付属セキュリティモジュール１２に記憶されている場合には、既に媒体付属セキュリティモジュール１２はＣＡ情報信号を持っている。そこで、媒体付属セキュリティモジュール１２では、ＣＡ情報信号を暗号復号し、利用条件を満足しているか否か判定した後、セキュリティモジュールインタフェース回路５を介して、媒体付属セキュリティモジュール１２から媒体付属セキュリティモジュール２２へ、当該番組ＣＡ情報信号の暗号復号鍵や資格情報の移動または複製を行なう。このとき必要に応じて、当該複写に伴う課金の情報をセキュリティモジュール６に記憶する。同時に、ＣＡ情報信号は、番組信号とともに記録媒体に記録されている場合には、番組信号と同じ経路で記録媒体１１から記録媒体２１に複写され、媒体付属セキュリティモジュールに記憶されている場合には、セキュリティモジュールインタフェース回路５を介して媒体付属セキュリティモジュール１２から媒体付属セキュリティモジュール２２に複写される。

【００２８】次に第３の実施例として、ＰＣ（パーソナルコンヒュータ）での記録や編集・表示などの利用をする場合について図６を用いて説明する。図１の基本構成において、記録・再生回路がＰＣインタフェース回路３１に、記録媒体がＰＣの記憶機能３３に、媒体付属セキュリティモジュールがＰＣ付属セキュリティモジュール３２にそれぞれ置き換わったものである。また、ＰＣ自身で表示したり編集したりすることが可能であるが、この場合に使用するデスクランブル機能３４および編集機能３５、提示機能３６が加わっている。ＰＣ（パーソナルコンピュータ）３０には、ＰＣインタフェース回路３１の一部ＰＣ付属セキュリティモジュール３２、記憶機能３３、デスクランブル機能３４、編集機能３５、提示機能３６が含まれる。なお、記憶機能３３、デスクランブル機能３４、編集機能３５、提示機能３６の各機能はＰＣのＣＰＵとソフトウェアによって実現される場合を含む。図６の構成において、記録・再生を行なう場合の動作は、実施例１における記録・再生回路をＰＣインタフェース回路３１に、記録媒体をＰＣの記憶機能３３に、媒体付属セキュリティモジュールをＰＣ付属セキュリティモジュール３２にそれぞれ置き換えたものと同様である。この時には、デスクランブル機能３４、編集機能３５、提示機能３６の各機能は動作に関係しない。

【００２９】また図６の構成においては、番組信号をＰＣ自身で表示したり編集したりすることも可能である。記憶機能３３から読み出されたスクランブルを施された番組信号は、ＰＣのデスクランブル機能３４によってスクランブルを解除され提示機能３６によって提示される。さらに、編集を行なう場合には、編集機能３５で編集した後再び提示機能３６によって提示したり、記憶機能３３に記憶したりする。このとき、ＰＣのデスクランブル機能３４におけるスクランブル解除に必要なスクランブル鍵は次のように得る。ＣＡ情報信号は番組信号とともに記憶機能３３から読み出され、ＰＣ付属セキュリティモジュール３２に渡される（ＣＡ情報信号が番組信号とともに記憶機能３３に記憶されている場合）か、または既にＰＣ付属セキュリティモジュール１２が記憶している（ＰＣ付属セキュリティモジュール１２に記憶さ

れている場合）。ＰＣ付属セキュリティモジュール３２では、ＣＡ情報信号を暗号復号し、利用条件を満足しているか否か判定した後にＰＣのデスクランブル機能３４に渡される。このときこの表示や編集に伴い課金が生じる場合には、ＰＣ付属セキュリティモジュール３２は、セキュリティモジュールインタフェース５を介してセキュリティモジュール６と通信し、課金情報をセキュリティモジュール６に記憶する。以上いくつかの実施例により本発明の実施の形態について詳細に説明してきたが、本発明はこれらの実施例に限定されることなく、発明の要旨内で各種の変形、変更が可能なことは自明である。

【００３０】

【発明の効果】本発明では、記録時および再生時における利用条件の検査を、ＣＰＵを内蔵したセキュリティモジュールあるいは媒体付属セキュリティモジュールにおいて行なうため、様々な利用条件を設定しそれに従って利用を制御したり課金したりすることが可能になる。例えば、次のような制御や課金が可能になる。

①予め利用回数を限定した記録とそれに対する課金
②予め利用期限を限定した記録とそれに対する課金
③予め複製個数を限定した記録とそれに対する課金
④利用条件を保留しての記録と実際に利用した時点での利用回数に応じた課金
⑤利用条件を保留しての記録と実際に複写した時点での複写個数に応じた課金
⑥予め複製個数や利用回数を限定して記録からの複製個数や利用回数の分配を受けての複製
⑦上記の組み合わせ。

【００３１】また、利用条件の検査はセキュリティモジュールまたは媒体付属セキュリティモジュール内部において行なわれるため、これらの処理は不正に対して安全である。例えば、仮に番組信号を記録された記録媒体の単純複製が可能であっても、スクランブル鍵情報や資格情報などを記憶した媒体付属セキュリティモジュールの複製は事実上不可能なので記録媒体カセットの不正複製、すなわち番組の不正複製は防止される。

【００３２】さらに、番組信号を記録した記録媒体と、その番組の利用資格を記録した媒体付属セキュリティモジュールは記録媒体カセットに一体化されて扱われるので、この記録媒体カセットさえ持っていれば、利用資格内で番組の利用が可能である。つまり、利用資格の制御を行ないながら、従来の記録媒体と同様に、移動、譲渡、貸し借りなどが可能な「もの」として扱うことができる。なお、記録媒体カセットの媒体付属セキュリティモジュールは、その記録媒体カセットの記録媒体に記録しただけの番組の利用資格を記録しさえすればよいので、記憶容量のオーバフローを計画的に防止することができる。

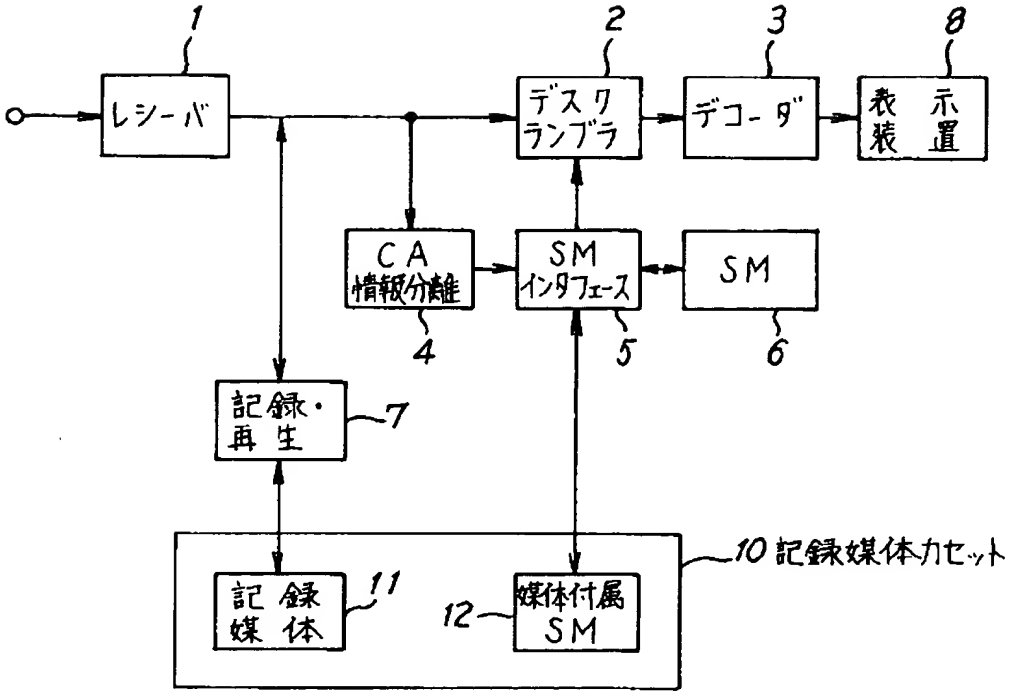
【図面の簡単な説明】

【図１】本発明の基本構成図である。
【図２】基本構成における通常視聴時の信号の流れを説明する図である。
【図３】基本構成における記録時の信号の流れを説明する図である。
【図４】基本構成における再生時の信号の流れを説明する図である。
【図５】第２の実施例の説明図である。
【図６】第３の実施例の説明図である。
【図７】第１の従来技術の説明図である。
【図８】第２の従来技術の説明図である。
【図９】第３の従来技術の説明図である。

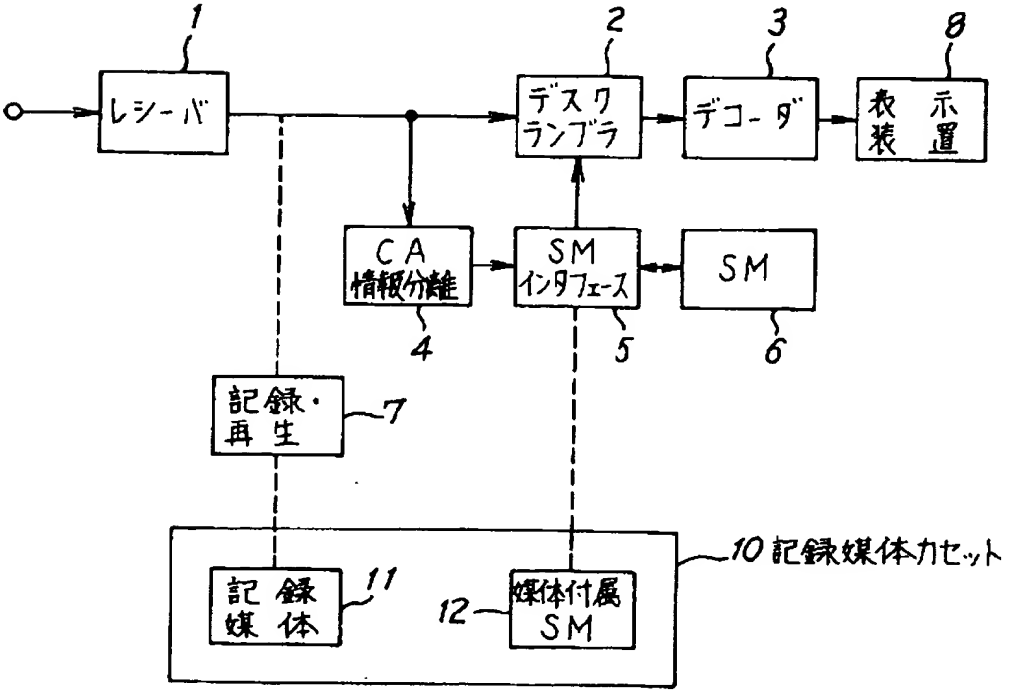
【符号の説明】

１　レシーバ回路
２　デスクランブラ回路
３　デコーダ回路
４　ＣＡ情報分離回路
５　セキュリティモジュールインタフェース回路
６　セキュリティモジュール
７　記録・再生回路
８　表示装置
９　ＣＧＭＳ制御回路
１０　記録媒体カセット
１１　記録媒体
１２　媒体付属セキュリティモジュール
１７　記録・再生回路
２０　記録媒体カセット
２１　記録媒体
２２　媒体付属セキュリティモジュール
３０　ＰＣ（パーソナルコンピュータ）
３１　ＰＣインタフェース
３２　ＰＣ付属セキュリティモジュール
３３　記憶機能
３４　デスクランブル機能
３５　編集機能
３６　提示機能

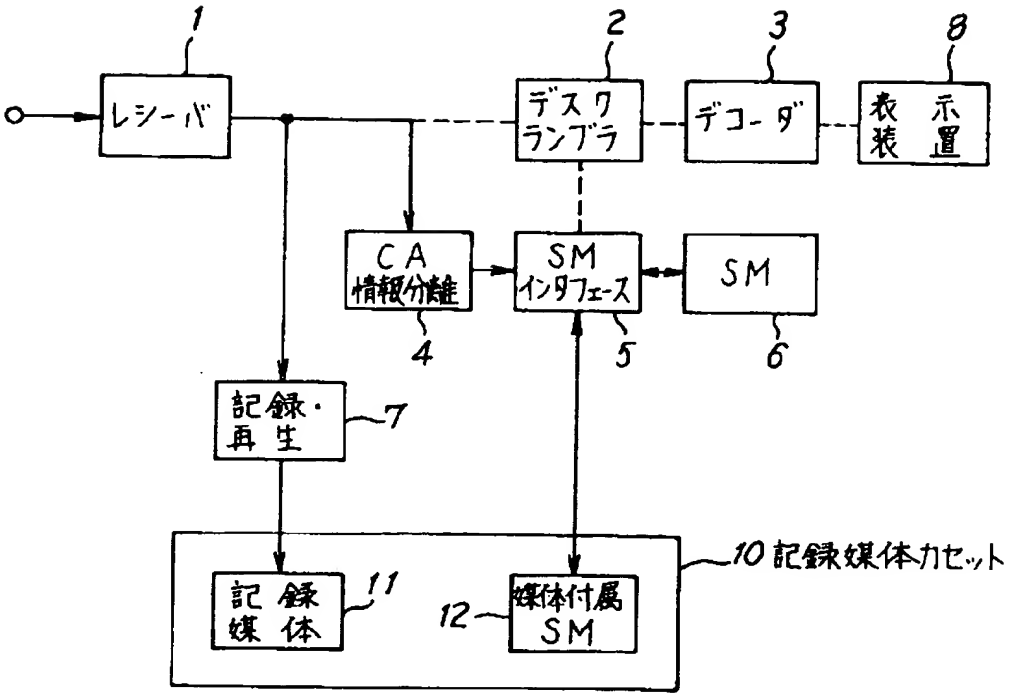
【図１】


1
2
3
8
レシーバ
デスクランブラ
デコーダ
表示装置
CA情報分離
SM インタフェース
SM
4
5
6
記録・再生
7
10 記録媒体カセット
記録媒体
11
12
媒体付属SM

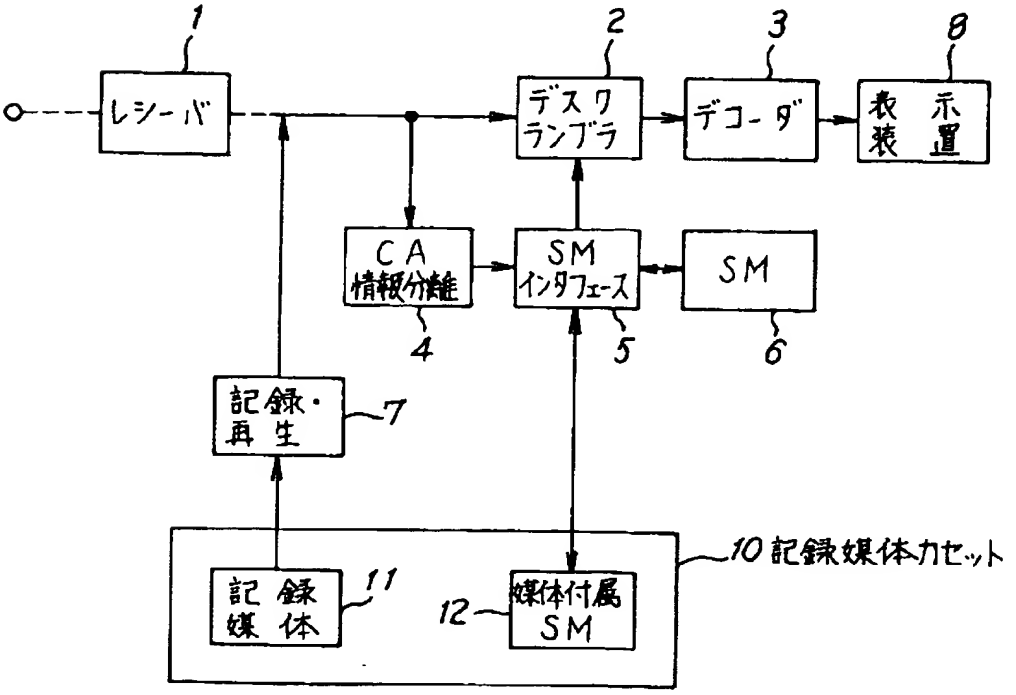
【図２】


1
2
3
8
レシーバ
デスクランブラ
デコーダ
表示装置
CA情報分離
SM インタフェース
SM
4
5
6
記録・再生
7
10 記録媒体カセット
記録媒体
11
12
媒体付属SM

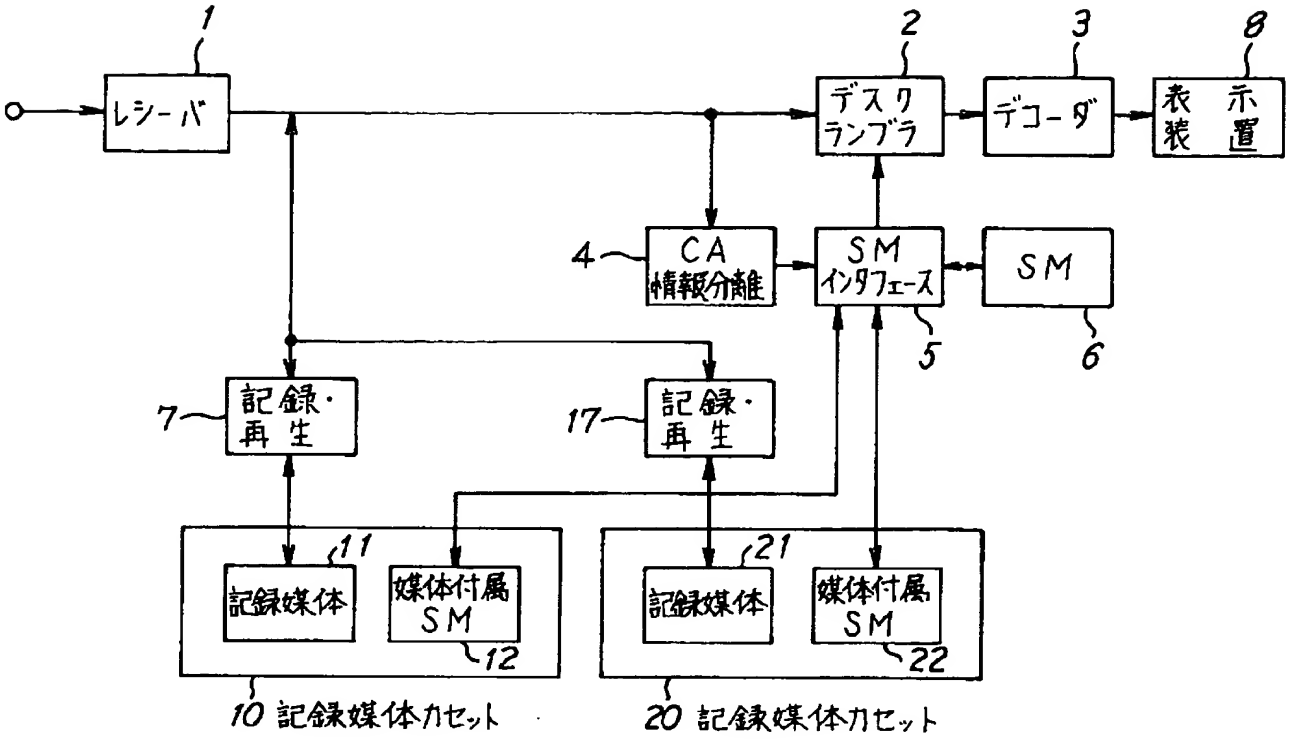
【図３】


1
2
3
8
レシーバ
デスクランブラ
デコーダ
表示装置
CA情報分離
SM インタフェース
SM
4
5
6
記録・再生
7
記録媒体
11
12
媒体付属SM
10 記録媒体カセット

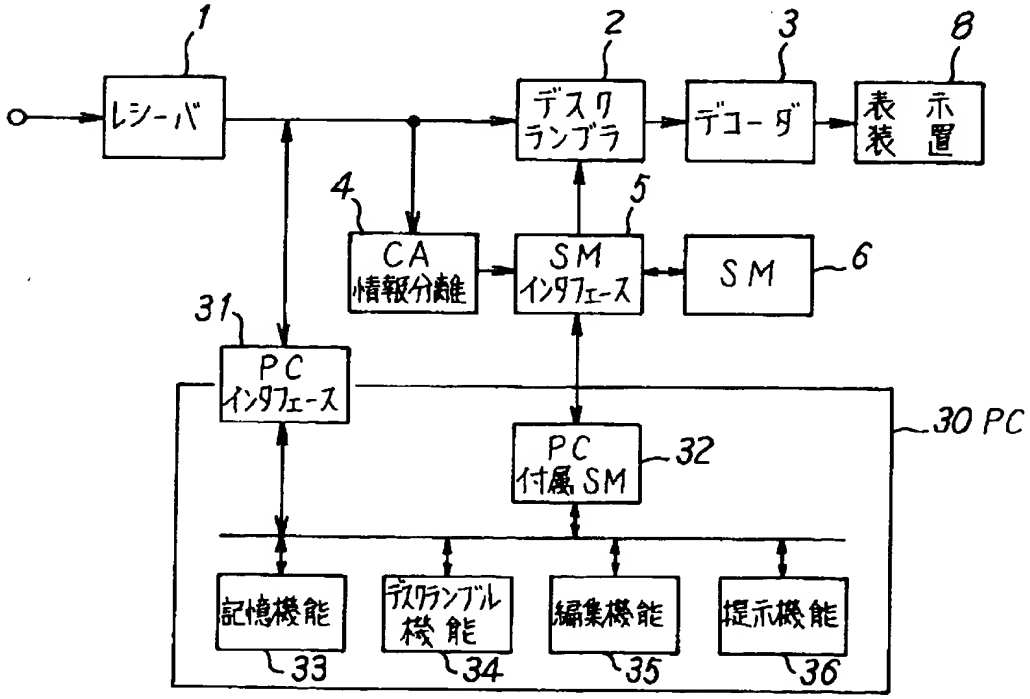
【図４】


1
2
3
8
レシーバ
デスクランブラ
デコーダ
表示装置
CA情報分離
SM インタフェース
SM
4
5
6
記録・再生
7
記録媒体
11
12
媒体付属SM
10 記録媒体カセット

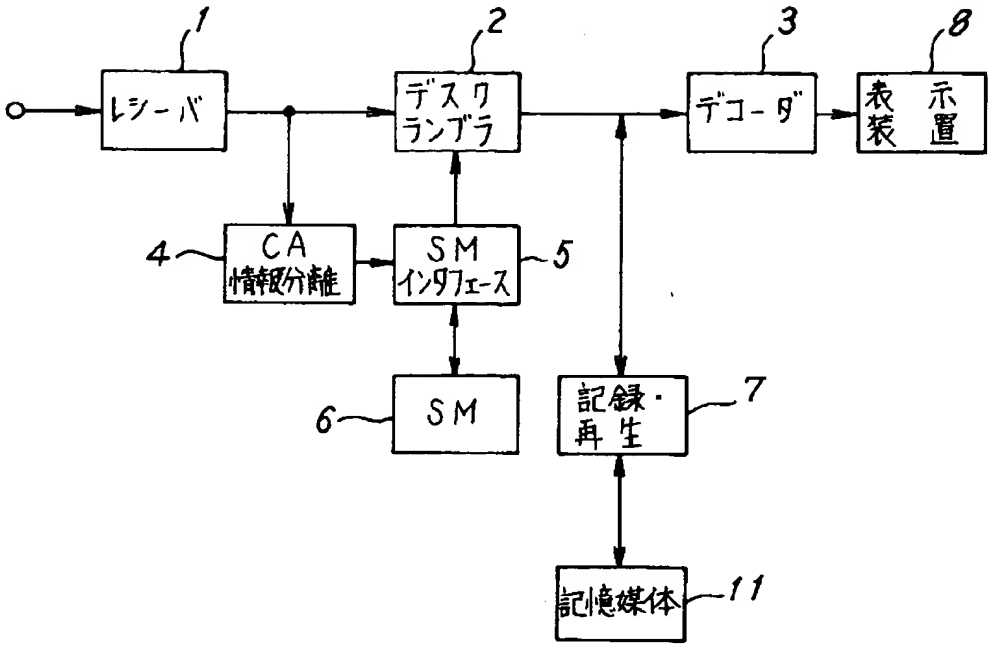
【図５】


1
レシーバ
2
デスクランブラ
3
デコーダ
8
表示装置
4
CA情報分離
SM インタフェース
5
SM
6
7
記録・再生
17
記録・再生
11
記録媒体
媒体付属SM
12
10 記録媒体カセット
21
記録媒体
媒体付属SM
22
20 記録媒体カセット

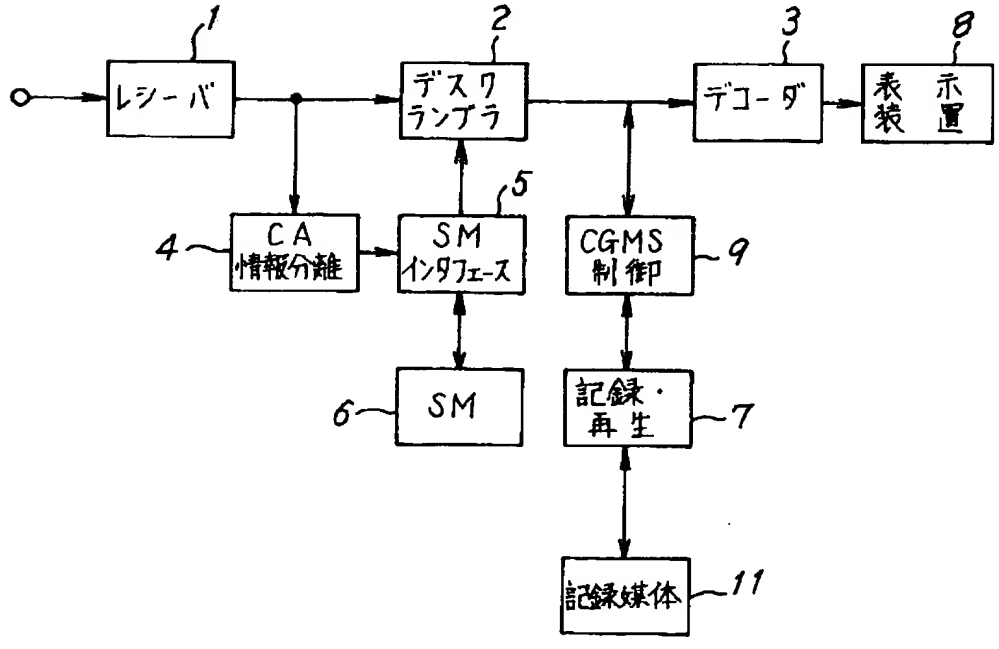
【図６】


1
レシーバ
2
デスクランブラ
3
デコーダ
8
表示装置
4
CA情報分離
5
SM インタフェース
SM
6
31
PC インタフェース
30 PC
PC付属SM
32
記憶機能
33
デスクランブル機能
34
編集機能
35
提示機能
36

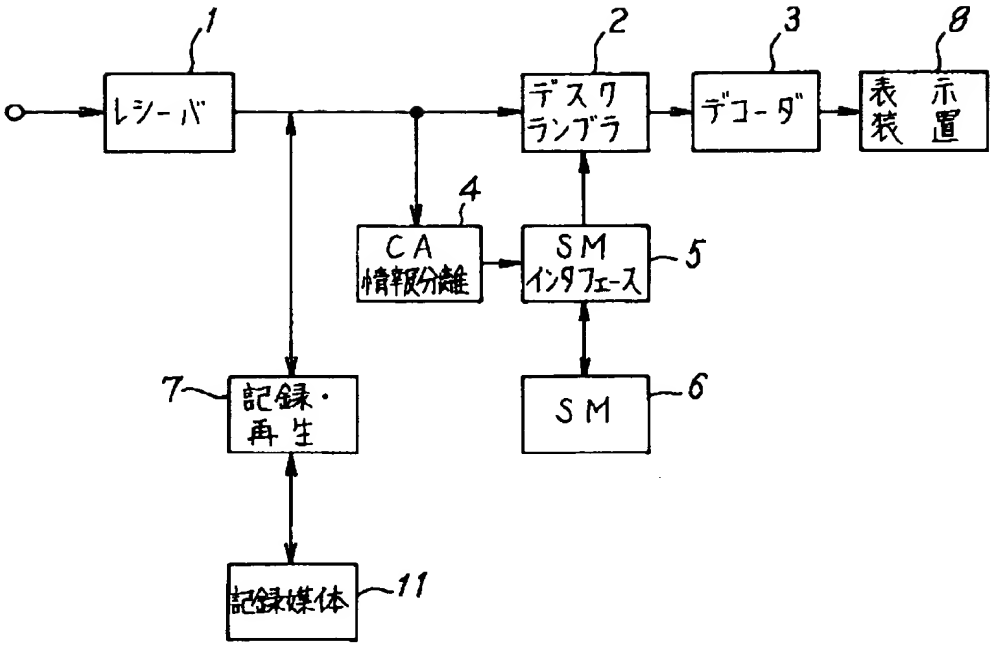
【図７】


1
2
3
8
レシーバ
デスクランブラ
デコーダ
表示装置
4
CA情報分離
SM インタフェース
5
6
SM
記録・再生
7
記憶媒体
11

【図８】


1
2
3
8
レシーバ
デスクランブラ
デコーダ
表示装置
5
4
CA情報分離
SM インタフェース
CGMS制御
9
6
SM
記録・再生
7
記録媒体
11

【図９】


1
レシーバ
2
デスクランブラ
3
デコーダ
8
表示装置
4
CA情報分離
SMインタフェース
5
7
記録・再生
SM
6
記録媒体
11